(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号
特開2001－177518
（P2001－177518A）
(43)公開日　平成13年６月29日(2001.6.29)

| (51)Int.Cl.[7] | 識別記号 | Ｆ Ｉ | テーマコード(参考) |
|---|---|---|---|
| Ｈ０４Ｌ　9/26 | | Ｇ０９Ｃ　1/00 | ６１０Ａ　５Ｊ１０４ |
| Ｇ０９Ｃ　1/00 | ６１０ | Ｈ０４Ｌ　9/00 | ６５９ |
| Ｈ０４Ｌ　9/14 | | | ６４１ |

審査請求　有　　請求項の数６　ＯＬ　（全　５　頁）

(21)出願番号　特願平11－360023

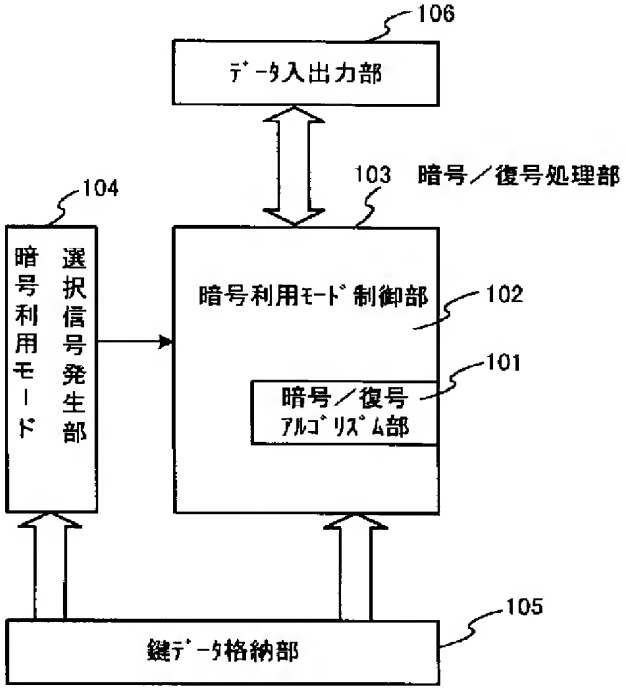
(22)出願日　平成11年12月17日(1999.12.17)

(71)出願人　000004237
日本電気株式会社
東京都港区芝五丁目７番１号
(72)発明者　田村　裕之
東京都港区芝五丁目７番１号　日本電気株式会社内
(74)代理人　100105511
弁理士　鈴木　康夫　（外１名）

Ｆターム(参考)　5J104 AA01 AA34 FA06 JA13 JA31 NA02

(54)【発明の名称】　暗号化方法、復号化方法及び装置

(57)【要約】
【課題】　暗号利用モードの設定による、より秘匿性の高い暗号化方法、復号化方法及び装置を提供する。
【解決手段】　鍵データ格納部１０５は、暗号利用モードを含む暗号鍵を格納する。暗号利用モード選択信号発生部１０４は、鍵データ格納部１０５から暗号鍵を読み出し、暗号利用モードを選択する選択信号を出力する。暗号利用モード制御部１０２は、前記選択信号により暗号／復号アルゴリズム部１０１の暗号利用モードを設定する。暗号／復号処理部１０３は、以上の設定によりデータ入出力部１０６からの平文又は暗号文のデータを暗号文又は平文のデータに変換して出力する。暗号鍵の中に暗号利用モード（連鎖技法）の情報を内蔵することにより、暗号化／復号化の暗号鍵に加えて暗号操作モードが設定されるので秘匿性を高めることができる。



1

【特許請求の範囲】

【請求項１】　暗号化及び復号化に共通鍵暗号を使用する暗号ブロック連鎖方式による暗号化方法において、暗号利用モードの設定情報を含む暗号鍵に基づいて、複数の異なる暗号ブロック連鎖による暗号化アルゴリズムが選択できる暗号化装置により、暗号利用モードの暗号化アルゴリズムの選択設定を行い、前記暗号鍵により暗号化を行うことを特徴とする暗号化方法。

【請求項２】　暗号化及び復号化に共通鍵暗号を使用する暗号ブロック連鎖方式による復号化方法において、暗号利用モードの設定情報を含む暗号鍵に基づいて、複数の異なる暗号ブロック連鎖による復号化アルゴリズムが選択できる復号化装置により、暗号利用モードの復号化アルゴリズムの選択設定を行い、前記暗号鍵により復号化を行うことを特徴とする復号化方法。

【請求項３】　共通鍵暗号方式の暗号鍵を格納する鍵データ格納部と、前記鍵データ格納部から暗号鍵を読み出し暗号鍵内の暗号利用モードを検出し暗号利用モードを選択する選択信号を出力する暗号利用モード選択信号発生部と、前記選択信号を入力し、複数の異なる暗号ブロック連鎖による暗号化アルゴリズムから前記選択信号で指定されている暗号利用モードの暗号化アルゴリズムを選択し、選択した暗号化アルゴリズムにより入力される平文のデータを暗号文のデータに変換して出力する暗号化処理部とを有することを特徴とする暗号化装置。

【請求項４】　共通鍵暗号方式の暗号鍵を格納する鍵データ格納部と、前記鍵データ格納部から暗号鍵を読み出し暗号鍵内の暗号利用モードを検出し暗号利用モードを選択する選択信号を出力する暗号利用モード選択信号発生部と、前記選択信号を入力し、複数の異なる暗号ブロック連鎖による復号化アルゴリズムから前記選択信号で指定されている暗号利用モードの復号化アルゴリズムを選択し、選択した復号化アルゴリズムにより入力される暗号文のデータを平文のデータに変換して出力する復号化処理部とを有することを特徴とする復号化装置。

【請求項５】　暗号利用モードとして、ＥＣＢ（Electric Code Book）モード、ＣＢＣ（Cipher Block Chaining）モード、ＣＦＢ（Cipher Feed Back）モード及びＯＦＢ（Output Feed Back）モードを選択することを特徴とする請求項３記載の暗号化装置。

【請求項６】　暗号利用モードとして、ＥＣＢ（Electric Code Book）モード、ＣＢＣ（Cipher Block Chaining）モード、ＣＦＢ（Cipher Feed Back）モード及びＯＦＢ（Output Feed Back）モードを選択することを特徴とする請求項４記載の復号化装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、暗号方式に関し、特に、暗号ブロック連鎖（連鎖技法）を利用した暗号化及び復号化方式に関する。

2

【０００２】

【従来の技術】従来、暗号方式として共通鍵暗号を使用する秘密鍵暗号方式ＤＳＥ（Data Encryption Standard）や公開鍵暗号方式ＲＳＡ（Rivest-Shamir-Adlemen）が知られている。これらの暗号方式では、平文をある一定のブロックに区切り、ブロック単位で公開鍵または秘密鍵によって暗号化することにより、最終的に平文全体を暗号化する。これらの暗号方式では、解読のされにくさを示す暗号強度が非常に高いとされているが、暗号化処理をブロック単位で行うため、平文の種類などによってはブロックごとに一定の統計的性質を示すことがあり、これが暗号強度を低下させる原因になりうる。

【０００３】このような暗号方式においては暗号化強度を高めるために、暗号ブロック連鎖方式が使用されている。暗号ブロック連鎖方式としては、ＩＳＯ８３７２において、ＣＢＣ（Cipher Block Chaining）、ＯＦＢ（Output Feed Back）、ＣＦＢ（Cipher Feed Back）及びＥＣＢ（Electric Code Book）の４種類の暗号モードが規定されている。前記モードＣＢＣ～ＣＦＢでは、一つの平文ブロックを暗号化するたびに、その結果または経過に基づく情報を暗号器にフィードバックさせ、その情報を次ブロック以降の暗号化に連鎖的に影響せしめる処理を行う。このため、これらの暗号モードによれば、あるブロックの暗号化が過去の暗号化処理の履歴に依存するため解読が困難になる。

【０００４】以上説明したように多くの共通鍵暗号方式において採用しているブロック暗号方式においては、その安全性を高めるために暗号利用モード（連鎖技法）が使用されている。この暗号利用モードは、暗号側及び復号側において同一に設定する必要がある。従来、暗号利用モードは独自の方法により暗号側及び復号側において固定的に設定して暗号化及び復号化を行うように構成した方式が採用されている。

【０００５】

【発明が解決しようとする課題】従来の暗号方式は、使用する暗号利用モードを固定的に設定して暗号化及び復号化を行うものであったが、必ずしも使用する暗号利用モードがそれぞれ完全な秘匿性を有するものではなから、固定的に特定の暗号利用モードを使用するだけでは秘匿性が充分でないという問題があった。

【０００６】（発明の目的）本発明の目的は、暗号利用モードの設定による、より秘匿性の高い暗号化方法、復号化方法及び装置を提供することにある。

【０００７】

【課題を解決するための手段】本発明の暗号化方法は、暗号化及び復号化に共通鍵暗号を使用する暗号ブロック連鎖方式による暗号化方法において、暗号利用モードの設定情報を含む暗号鍵に基づいて、複数の異なる暗号ブロック連鎖による暗号化アルゴリズムが選択できる暗号化装置により、暗号利用モードの暗号化アルゴリズムの

設定を行い、前記暗号鍵により暗号化を行うことを特徴とする。また、本発明の復号化方法は、暗号化及び復号化に共通鍵暗号を使用する暗号ブロック連鎖方式による復号化方法において、暗号利用モードの設定情報を含む暗号鍵に基づいて、複数の異なる暗号ブロック連鎖による復号化アルゴリズムが選択できる復号化装置により、暗号利用モードの復号化アルゴリズムの設定を行い、前記暗号鍵により復号化を行うことを特徴とする。

【０００８】本発明の暗号化装置は、共通鍵暗号方式の暗号鍵を格納する鍵データ格納部と、前記鍵データ格納部から暗号鍵を読み出し暗号鍵内の暗号利用モードを検出し暗号利用モードを選択する選択信号を出力する暗号利用モード選択信号発生部と、前記選択信号を入力し、複数の異なる暗号ブロック連鎖による暗号化アルゴリズムから前記選択信号で指定されている暗号利用モードの暗号化アルゴリズムを選択し、選択した暗号化アルゴリズムにより入力される平文のデータを暗号文のデータに変換して出力する暗号化処理部とを有することを特徴とする。また、本発明の復号化装置は、共通鍵暗号方式の暗号鍵を格納する鍵データ格納部と、前記鍵データ格納部から暗号鍵を読み出し暗号鍵内の暗号利用モードを検出し暗号利用モードを選択する選択信号を出力する暗号利用モード選択信号発生部と、前記選択信号を入力し、複数の異なる暗号ブロック連鎖による復号化アルゴリズムから前記選択信号で指定されている暗号利用モードの復号化アルゴリズムを選択し、選択した復号化アルゴリズムにより入力される暗号文のデータを平文のデータに変換して出力する復号化処理部とを有することを特徴とする。

【０００９】本発明の暗号利用モードとしては、ＥＣＢ（Electric Code Book）モード、ＣＢＣ（Cipher Block Chaining）モード、ＣＦＢ（Cipher Feed Back）モード及びＯＦＢ（Output Feed Back）モードが利用される。

【００１０】本発明では、元来秘匿性が保証され、また暗号側／復号側にて共有する暗号鍵に暗号利用モードの情報を内蔵させ、この情報により暗号操作モードの設定を行う。一般的に知られる共通鍵暗号方式において、暗号鍵の中に暗号利用モード（連鎖技法）の情報を内蔵させることにより、より秘匿性の高い暗号化方法、復号化方法及び装置を構成できる。

【００１１】（作用）暗号鍵の中に暗号利用モード（連鎖技法）の情報を内蔵させることにより、暗号化／復号化における暗号鍵に加えて暗号操作モードを設定できるから、秘匿性を一層高めることが可能である。

【００１２】

【発明の実施の形態】（構成の説明）図１は、本発明の暗号化方法、復号化方法及び装置の一実施の形態を示すブロック図である。暗号／復号アルゴリズム部１０１、暗号利用モード制御部１０２からなる暗号／復号処理部１０３、暗号利用モード選択信号発生部１０４、鍵データ格納部１０５及びデータ入出力部１０６から構成される。各部の機能概要は次のとおりである。

【００１３】鍵データ格納部１０５は、暗号利用モードの符号を含む暗号鍵のデータ（鍵データ）を記憶する機能を有する。暗号利用モード選択信号発生部１０４は、鍵データ格納部１０５に格納されている鍵データを読み出し鍵データに含まれる暗号鍵の暗号利用モードの符号を検出し、暗号／復号アルゴリズムを選択する選択信号を生成し、暗号／復号処理部１０３に出力する機能を有する。

【００１４】暗号／復号処理部１０３は、鍵データ格納部１０５から暗号／復号のための暗号化・復号化の鍵データを入力するとともに、データ入出力部１０６からのデータを入力し、入力したデータを暗号化又は復号化してデータ入出力部１０６に出力する機能を有する。暗号／復号処理部１０３は、暗号／復号アルゴリズム部１０１と暗号利用モード制御部１０２とから構成されており、暗号利用モード制御部１０２は、暗号利用モード選択信号発生部１０４からの前記選択信号に基づき、暗号／復号アルゴリズム部１０１の実行するアルゴリズムを指定する機能を有し、暗号／復号アルゴリズム部１０１は、複数の暗号／復号アルゴリズムを実行する機能を有し、暗号利用モード制御部１０２から指定されたアルゴリズムによりデータの暗号化又は復号化を実行する。

【００１５】図２は、本実施の形態において使用する暗号利用モードの例を示すブロック図である。同図では説明上、暗号化（装置）及び復号化（装置）を直列接続した構成により暗号利用モードの機能構成を示している。本実施の形態では、暗号／復号アルゴリズム部１０１の複数の暗号／復号アルゴリズムとして、ＥＣＢ（Electric Code Book）モード２０１、ＣＢＣ（Cipher Block Chaining）モード２０２、ＣＦＢ（Cipher Feed Back）モード２０３及びＯＦＢ（Output Feed Back）モード２０４の４つの暗号／復号アルゴリズムを処理する機能を備えるものとしている。

【００１６】ここで、ＥＣＢモード２０１は、平文を暗号鍵によりＥＣＢの暗号文へ暗号化し、また、ＥＣＢの暗号文を暗号鍵により平文に復号化する暗号利用モードである。ＣＢＣモード２０２は、暗号利用モードとしてサイファーブロック連鎖（Cipher Block Chaining）モードを使用するものであり、平文を暗号鍵により暗号化した１ブロックの暗号文を遅延して帰還し、次のブロックとの排他的論理和演算を行う。同様にして、次のブロックはその直前のブロックと暗号化データとの排他的論理和演算を行うように順次処理を繰り返し、各暗号文のブロックは直前までの平文ブロック及び暗号鍵に依存するような暗号化を行う。復号化においては、暗号鍵により復号化し１ブロック前の暗号文と排他的論理和演算を行うことにより平文に復号化する。

【００１７】また、ＣＦＢ（Cipher Feed Back）モード２０３では、暗号化において暗号文を１ブロック単位で暗号鍵により暗号化し次の平文との排他的論理和演算を行う処理を繰り返し、復号化においては、１ブロック前の暗号文と暗号鍵により復号化したものとの排他的論理和演算を行って平文に復号する。更に、ＯＦＢ（Output Feed Back）モード２０４では、１ブロック単位で暗号鍵を繰り返し暗号化処理を行うとともに平文との排他的論理和演算を行うことで暗号化して暗号文を生成する。復号化においても同様に暗号鍵に繰り返しの暗号化処理を行うと共に暗号文との排他的論理和演算を行って平文に復号する。

【００１８】図３は、暗号鍵（鍵データ）の内容及び暗号利用モードの選択設定の一例を示す図である。ｎ＋１ビットの鍵データ中に暗号利用モードの選択用の設定ビットを設け、この設定ビットにより複数の暗号／復号アルゴリズムの何れかを設定する。

【００１９】（動作の説明）次に、本実施の形態の暗号化方法、復号化方法及び装置の動作について図面を参照して説明する。

【００２０】鍵データ格納部（１０５）には、実際の暗号／復号処理を行う前に、使用する鍵データが格納される。ここで、鍵データは図３に示すようにｂ０からｂｎまでのｎ＋１ビットでなり、ｂ２からｂｎまでのビットは暗号利用モードの暗号化／復号化アルゴリズムのデータとし、ｂ０及びｂ１を暗号利用モードの設定ビットとすることができる。本実施の形態では、２ビットデータ（０、０）、（０、１）、（１、０）及び（１、１）により、４つの暗号利用モードＥＣＢ、ＣＢＣ、ＣＦＢ及びＯＦＢを設定することを可能としている。また、暗号利用モードの暗号化／復号化アルゴリズムのデータをｂ０からｂｎまでとし、ｂ０及びｂ１は暗号利用モードを指定するビットとしての情報も有するようにすることもできる。

【００２１】暗号利用モード選択信号発生部（１０４）と暗号／復号処理部（１０３）は、それぞれ前記鍵データ格納部（１０５）に記憶された鍵データを読み出す。暗号利用モード選択信号発生部（１０４）は、読み出した鍵データから暗号利用モード設定ビットを抽出して選択信号を生成し、暗号利用モード制御部（１０２）に選択信号を送出する。暗号／復号処理部（１０３）は、前記鍵データと前記選択信号とを入力し、暗号利用モード制御部（１０２）において、前記選択信号により設定された暗号操作モードに対応したデータパス（ＬＯＯＰ制御）を形成する。ここで、暗号利用モードは、平文から暗号文、暗号文から平文を抽出することができるように暗号側／復号側にて同一に設定される。

【００２２】このようにして形成された暗号化及び復号化構成をもつ暗号／復号処理部（１０３）に、データ入出力部（１０６）を介して、暗号／復号データが入力され、暗号／復号処理済みデータがデータ入出力部（１０６）を介して出力される。

【００２３】（他の実施の形態）以上説明した実施の形態では、暗号利用モードの設定を暗号鍵の末尾の２ビット（「０」、「１」）を暗号側／復号側において抽出して使用するように構成しているが、暗号鍵の中から任意のｍ（ｍ＜ｎ）ビットを特定してあらかじめ定めておくようにすることができる。また、この暗号利用モードの設定用のビットは暗号鍵の一部とすることも独立した専用ビットとすることも可能である。

【００２４】また、前記実施の形態において、暗号／復号アルゴリズム部１０１及び暗号利用モード制御部１０２からなる暗号／復号処理部１０３は、暗号化及び復号化を行う機能を有することとし、データ入出力部１０６は平文又は暗号文を変換処理のために出力し、変換処理により生成されたそれぞれ暗号文又は平文を入力する機能を有することとしたが、それぞれ暗号化又は復号化の何れかの機能を有する構成とすることができる。また、データ入出力部１０６はデータ入力部とデータ出力部とに独立した構成とすることができることは云うまでもない。

【００２５】

【発明の効果】本発明によれば、暗号利用モードの設定を暗号鍵により行うように構成しているので、暗号鍵の設定により同時に暗号利用モードが設定されるので、暗号の秘匿性を充分高めることが可能である。

【００２６】また、暗号側、復号側にて共通の鍵データを所有（鍵配送）するための共通鍵暗号方式における鍵データに暗号利用モードの設定情報を含めているので、鍵配送のシステムに新たな手順又は手段を加える必要がないという利点がある。

【図面の簡単な説明】

【図１】本発明の暗号化及び復号化の一実施の形態を示す図である。

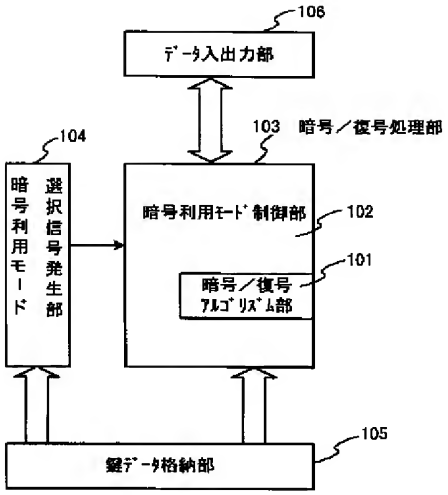
【図２】本実施の形態において利用する暗号利用モードを示す図である。

【図３】鍵データの内容及び暗号利用モードの選択設定の一例を示す図である。

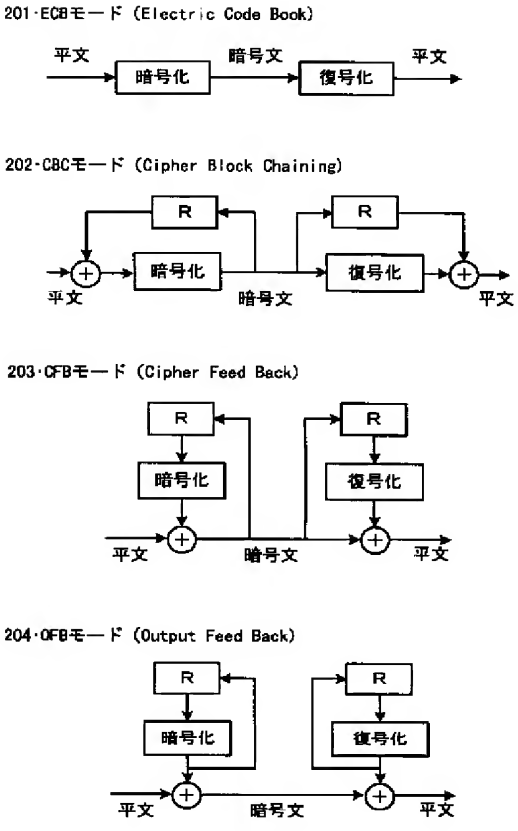
【符号の説明】

１０１　暗号／復号アルゴリズム部
１０２　暗号利用モード制御部
１０３　暗号／復号処理部
１０４　暗号利用モード選択信号発生部
１０５　鍵データ格納部
１０６　データ入出力部
２０１　ＥＣＢモード
２０２　ＣＢＣモード
２０３　ＣＦＢモード
２０４　ＯＦＢモード

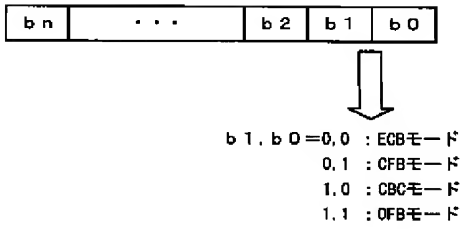
【図１】


106
データ入出力部
103　暗号／復号処理部
104
暗号利用モード
選択信号発生部
暗号利用モード制御部
102
101
暗号／復号アルゴリズム部
105
鍵データ格納部

【図２】


201･ECBモード（Electric Code Book）
平文
暗号化
暗号文
復号化
平文
202･CBCモード（Cipher Block Chaining）
R
暗号化
復号化
平文
暗号文
平文
203･CFBモード（Cipher Feed Back）
R
暗号化
復号化
平文
暗号文
平文
204･OFBモード（Output Feed Back）
R
暗号化
復号化
平文
暗号文
平文

【図３】


ｂｎ
・・・
ｂ２
ｂ１
ｂ０
ｂ１，ｂ０＝0,0　：ECBモード
0,1　：CFBモード
1,0　：CBCモード
1,1　：OFBモード

## FULL CONTENTS

[Claim(s)]

[Claim 1] In the encryption method by cipher block chaining which uses a common key code for encryption and a decoding The encryption method characterized by performing selection setting of the encryption algorithm in code use mode, and enciphering with said cryptographic key with the encryption equipment which can choose the encryption algorithm by several different code block chaining based on the cryptographic key including the setup information in code use mode.

[Claim 2] In the decoding method by cipher block chaining which uses a common key code for encryption and a decoding The decoding method characterized by performing selection setting of the decoding algorithm in code use mode, and decrypting with said cryptographic key with the decoding equipment which can choose the decoding algorithm by several different code block chaining based on the cryptographic key including the setup information in code use mode.

[Claim 3] The lock data storing section which stores the cryptographic key of a common key encryption system, and the code use mode selection-signal generating section which outputs the selection signal which reads a cryptographic key from said lock data storing section, detects the code use mode in a cryptographic key, and chooses code use mode, Input said selection signal and the encryption algorithm in the code use mode specified with said selection signal is chosen from the encryption algorithm by several different code block chaining. Encryption equipment characterized by having the encryption processing section which changes and outputs the data of a plaintext inputted by the selected encryption algorithm to the data of a cipher.

[Claim 4] The lock data storing section which stores the cryptographic key of a common key encryption system, and the code use mode selection-signal generating section which outputs the selection signal which reads a cryptographic key from said lock data storing section,

detects the code use mode in a cryptographic key, and chooses code use mode, Input said selection signal and the decoding algorithm in the code use mode specified with said selection signal is chosen from the decoding algorithm by several different code block chaining. Decoding equipment characterized by having the decoding processing section which changes and outputs the data of a cipher inputted by the selected decoding algorithm to the data of a plaintext.

[Claim 5] As code use mode, ECB (Electric Code Book) mode, Encryption equipment according to claim 3 characterized by choosing the CBC (Cipher Block Chaining) mode, CFB (Cipher Feed Back) mode, and OFB (Output Feed Back) mode.

[Claim 6] As code use mode, ECB (Electric Code Book) mode, Decoding equipment according to claim 4 characterized by choosing the CBC (Cipher Block Chaining) mode, CFB (Cipher Feed Back) mode, and OFB (Output Feed Back) mode.

---

[Detailed Description of the Invention]

[0001]

[Field of the Invention] Especially this invention relates to the encryption and the decoding system using code block chaining (chain technique) about a cipher system.

[0002]

[Description of the Prior Art] The secret key cryptosystem DSE (Data Encryption Standard) and the public key cryptosystem RSA (Rivest-Shamir-Adlemen) which use a common key code as a cipher system are known conventionally. Finally in these cipher systems, the whole plaintext is enciphered by dividing a plaintext into a certain fixed block, and enciphering with a public key or a secret key by a block unit. In these cipher systems, if the cryptographic strength which decode is carried out and shows hard is very high, it is carried out, but since encryption processing is performed by a block unit, it can become the cause by which the kind of plaintext etc. may show a fixed statistical property for every block, and this reduces cryptographic strength.

[0003] In order to raise encryption intensity in such a cipher system, cipher block chaining is used. As cipher block chaining, in ISO8372, CBC (Cipher Block Chaining), Four kinds of code modes of OFB (Output Feed Back), CFB (Cipher Feed Back), and ECB (Electric Code Book) are specified. In said mode CBC-CFB, the information based on [ whenever it enciphers one plaintext block ] the result or progress is made to feed back to a code machine, and processing which makes the information influence the encryption after a following block continuously is performed. For this reason, according to such code modes, decode becomes difficult in order that encryption of a certain block may be dependent on the history of the past encryption

processing.
[0004] As explained above, in order to raise the safety in the block cipher system adopted in many common key encryption systems, code use mode (chain technique) is used. It is necessary to set this code use mode to the code and decode side identically. The method constituted so that code use mode might be set to the code and decode side fixed by an original method and encryption and a decoding might be performed conventionally is adopted.
[0005]
[Problem to be solved by the invention] [ the cipher system ] although the conventional cipher system set up the code use mode to be used fixed and performed encryption and a decoding in some which have privacy with respectively perfect code use mode used not necessarily, there was a problem that privacy was not enough, only by using specific code use mode fixed inside.
[0006] (The purpose of invention) The purpose of this invention is to offer the high encryption method of privacy by setup in code use mode, the decoding method, and equipment more.
[0007]
[Means for solving problem] In the encryption method by cipher block chaining with which the encryption method of this invention uses a common key code for encryption and a decoding Based on the cryptographic key including the setup information in code use mode, with the encryption equipment which can choose the encryption algorithm by several different code block chaining, encryption algorithm in code use mode is set up and it is characterized by enciphering with said cryptographic key. Moreover, the decoding method of this invention is set to the decoding method by cipher block chaining which uses a common key code for encryption and a decoding. Based on the cryptographic key including the setup information in code use mode, with the decoding equipment which can choose the decoding algorithm by several different code block chaining, the decoding algorithm in code use mode is set up and it is characterized by decrypting with said cryptographic key.
[0008] The lock data storing section in which the encryption equipment of this invention stores the cryptographic key of a common key encryption system, The code use mode selection-signal generating section which outputs the selection signal which reads a cryptographic key from said lock data storing section, detects the code use mode in a cryptographic key, and chooses code use mode, Input said selection signal and the encryption algorithm in the code use mode specified with said selection signal is chosen from the encryption algorithm by several different code block chaining. It is characterized by having the encryption processing section which changes and outputs the data of a plaintext inputted by the selected encryption algorithm to the data of a cipher. Moreover, the lock data storing section in which the decoding equipment of this invention stores the cryptographic key of a common key encryption system, The code use mode selection-signal generating section which outputs the selection signal

which reads a cryptographic key from said lock data storing section, detects the code use mode in a cryptographic key, and chooses code use mode, Input said selection signal and the decoding algorithm in the code use mode specified with said selection signal is chosen from the decoding algorithm by several different code block chaining. It is characterized by having the decoding processing section which changes and outputs the data of a cipher inputted by the selected decoding algorithm to the data of a plaintext.

[0009] As code use mode of this invention, ECB (Electric Code Book) mode, The CBC (Cipher Block Chaining) mode, CFB (Cipher Feed Back) mode, and OFB (Output Feed Back) mode are used.

[0010] In this invention, the information on code use mode is made to build in the cryptographic key which privacy is originally guaranteed and is shared between the code side / decode side, and the code operation mode is set up using this information. In the common key encryption system generally known, the high encryption method, the decoding method, and equipment of privacy can be constituted more by making the information on code use mode (chain technique) build in in a cryptographic key.

[0011] (OPERATION) Since the code operation mode can be set up by making the information on code use mode (chain technique) build in in a cryptographic key in addition to the cryptographic key in encryption/decoding, it is possible to raise privacy further.

[0012]

[Mode for carrying out the invention] (Explanation of composition) Drawing 1 is the block diagram showing the form of 1 operation of the encryption method of this invention, the decoding method, and equipment. It consists of a code / decode algorithm section 101, the code / decoding processing section 103 that consists of a code use mode controller 102, the code use mode selection-signal generating section 104, the lock data storing section 105, and data I/O 106. The functional description of each part is as follows.

[0013] The lock data storing section 105 has the function to memorize the data (lock data) of the cryptographic key containing the sign in code use mode. The code use mode selection-signal generating section 104 detects the sign in the code use mode of the cryptographic key which reads the lock data stored in the lock data storing section 105, and is contained in lock data, generates the selection signal which chooses a code / decode algorithm, and has the function outputted to a code / decoding processing section 103.

[0014] A code / decoding processing section 103 has the function which inputs the data from the data I/O 106, enciphers or decrypts the inputted data, and is outputted to the data I/O 106 while inputting the lock data of the encryption and the decoding for a code/decode from the lock data storing section 105. A code / decoding processing section 103 consists of a code / the decode algorithm section 101, and a code use mode controller 102, and [ the code use mode controller 102 ] It is based on said selection signal from the code use mode selection-

signal generating section 104. Have the function to specify the algorithm which a code / decode algorithm section 101 performs, and [ a code / decode algorithm section 101 ] It has the function to perform two or more code / decode algorithms, and a data encryption or a decoding is performed by the algorithm specified from the code use mode controller 102.
[0015] Drawing 2 is the block diagram showing the example in the code use mode used in the form of this operation. In this figure, the composition which carried out series connection of encryption (equipment) and the decoding (equipment) shows the functional constitution in code use mode on explanation. With the form of this operation, as two or more code / decode algorithms of a code / decode algorithm section 101 The ECB (Electric Code Book) mode 201, the CBC (Cipher Block Chaining) mode 202, the CFB (Cipher Feed Back) mode 203, and OFB (Output) It shall have the function to process four the code / decode algorithms in the Feed Back mode 204.
[0016] Here, the ECB mode 201 is code use mode which enciphers a plaintext to the cipher of ECB with a cryptographic key, and decrypts the cipher of ECB to a plaintext with a cryptographic key. The CBC mode 202 uses Sypher block-chaining (Cipher Block Chaining) mode as code use mode, delays and returns the 1-block cipher which enciphered the plaintext with the cryptographic key, and performs EXCLUSIVE OR operation with the next block. Similarly, the next block repeats sequential operation so that EXCLUSIVE OR operation of the block in front of that and encryption data may be performed, and the block of each cipher performs encryption which is dependent on the plaintext block of a just before, and a cryptographic key. In a decoding, it decrypts to a plaintext by decrypting with a cryptographic key and performing the cipher and EXCLUSIVE OR operation before 1 block.
[0017] moreover, in the CFB (Cipher Feed Back) mode 203 The processing which enciphers a cipher with a cryptographic key by 1 block unit in encryption, and performs EXCLUSIVE OR operation with the following plaintext is repeated, EXCLUSIVE OR operation of the cipher in front of 1 block and the thing decrypted with the cryptographic key is performed in a decoding, and it decodes to a plaintext. Furthermore, in the OFB (Output Feed Back) mode 204, while repeating a cryptographic key by 1 block unit and performing encryption processing, it enciphers by performing EXCLUSIVE OR operation with a plaintext, and a cipher is generated. While performing repeated encryption processing to a cryptographic key similarly in a decoding, EXCLUSIVE OR operation with a cipher is performed and it decodes to a plaintext.
[0018] Drawing 3 is the figure showing an example of the contents of the cryptographic key (lock data), and the selection setting in code use mode. Into n+1-bit lock data, the setting bit for selection in code use mode is prepared, and it is set up by this setting bit any of two or more code / decode algorithms they are.
[0019] (Explanation of operation) Next, operation of the encryption method of the form this operation, the decoding method, and equipment is explained with reference to Drawings.

[0020] Before performing actual code/decoding processing, the lock data to be used is stored in the lock data storing section (105). Here, lock data becomes at n+1 bit from b0 to bn, as shown in drawing 3 , and the bit from b2 to bn can be used as the data of encryption/decoding algorithm in code use mode, and can make b0 and b1 the setting bit in code use mode. With the form of this operation, it makes it possible to set up 2 bit data (0, 0), (0, 1), and (1, 0) (1, 1) four code use modes ECB, CBC, CFB, and OFB. Moreover, the data of encryption/decoding algorithm in code use mode is carried out to from b0 to bn, and b0 and b1 can also have the information as a bit that code use mode is specified.

[0021] The code use mode selection-signal generating section (104), and a code / decoding processing section (103) read the lock data memorized by said lock data storing section (105), respectively. The code use mode selection-signal generating section (104) extracts a code use mode setting bit from the read lock data, generates a selection signal, and sends out a selection signal to a code use mode controller (102). A code / decoding processing section (103) inputs said lock data and said selection signal, and forms the data path (LOOP control) corresponding to the code operation mode set up by said selection signal in a code use mode controller (102). Here, from a plaintext, code use mode is identically set up at the code side / decode side so that a plaintext can be extracted from a cipher and a cipher.

[0022] Thus, a code/decode data is inputted into a code / decoding processing section with the encryption and decoding composition which were formed (103) through data I/O (106), and a code / decoding processing finishing data is outputted to it through data I/O (106).

[0023] (Form of other operations) [ constitute a setup in code use mode from a form of the operation explained above so that 2 bits ("0", "1") of the tail of a cryptographic key may be extracted and used for the code side / decode side, but ] Out of the cryptographic key, arbitrary m (m<n) bits are specified and it can set beforehand. Moreover, the bit for a setup in this code use mode can also be considered [ also supposing a part / a cryptographic key / or ] as the independent exclusive bit.

[0024] [ moreover, the code / decoding processing section 103 which consists of a code / the decode algorithm section 101, and a code use mode controller 102 in the form of said operation ] Although we decided to have the function to perform encryption and a decoding and it has the function which the data I/O 106 outputted the plaintext or the cipher for transform processing, and was generated by transform processing to input a cipher or a plaintext, respectively It can have composition which has which function of encryption or a decoding, respectively. Moreover, the data I/O 106 does not need to say that it can have composition which became independent in the data input section and the data output section.

[0025]

[Effect of the Invention] Since according to this invention it constitutes so that code use mode may be set up with a cryptographic key and code use mode is simultaneously set up by setup

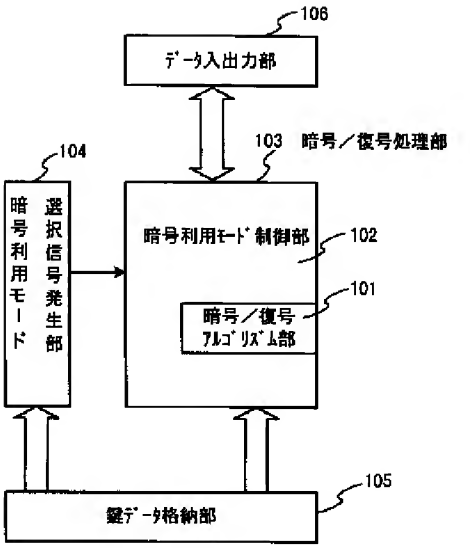
of a cryptographic key, it is possible to raise the privacy of a code enough.
[0026] Moreover, since the setup information in code use mode is included in the lock data in the common key encryption system for owning lock data common to the code and decode side (key delivery), there is an advantage that it is not necessary to add a new procedure or a new means to the system of key delivery.

---

[Brief Description of the Drawings]
[Drawing 1] It is the figure showing the form of 1 implementation of encryption of this invention, and a decoding.
[Drawing 2] It is the figure showing the code use mode used in the form of this operation.
[Drawing 3] It is the figure showing an example of the contents of lock data, and the selection setting in code use mode.
[Explanations of letters or numerals]
101 Code / Decode Algorithm Section
102 Code Use Mode Controller
103 Code / Decoding Processing Section
104 Code Use Mode Selection-Signal Generating Section <BR> 105 Lock Data Storing Section
106 Data I/O
201 ECB Mode
202 CBC Mode
203 CFB Mode
204 OFB Mode

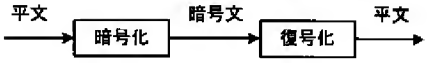
---

[Drawing 1]

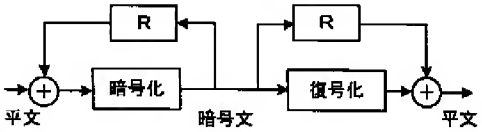



[Drawing 2]

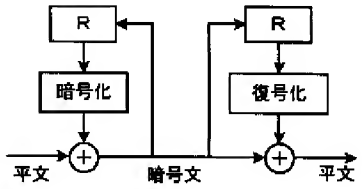
201-ECBモード (Electric Code Book)



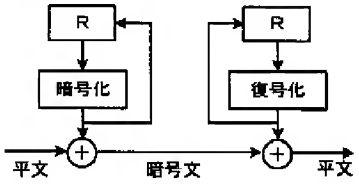

202-CBCモード (Cipher Block Chaining)



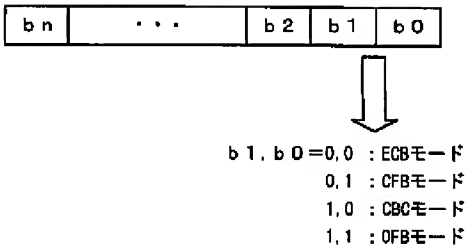

203-CFBモード (Cipher Feed Back)




204-OFBモード (Output Feed Back)




[Drawing 3]




[Translation done.]